ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

# Algorithms for Radio Networks

## Network Coding

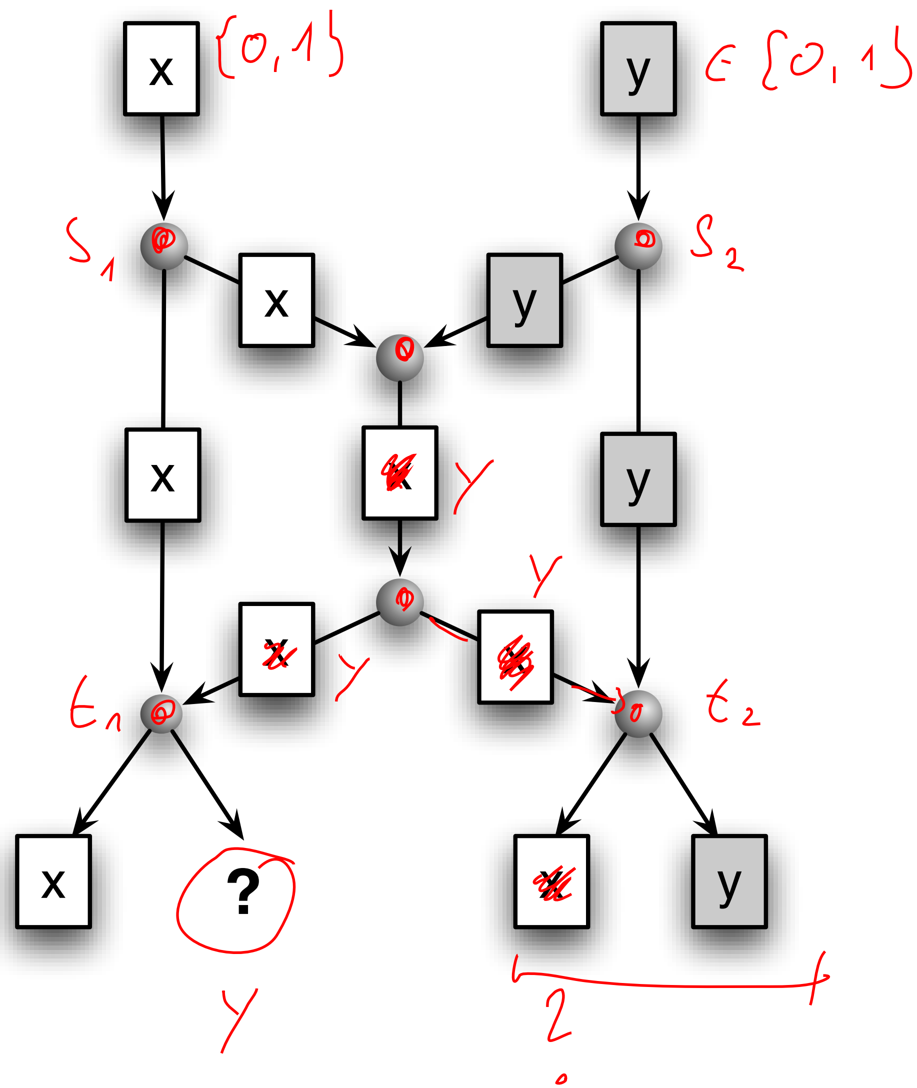
University of Freiburg
Technical Faculty
Computer Networks and Telematics
Christian Schindelhauer

CoNe Freiburg

IIF

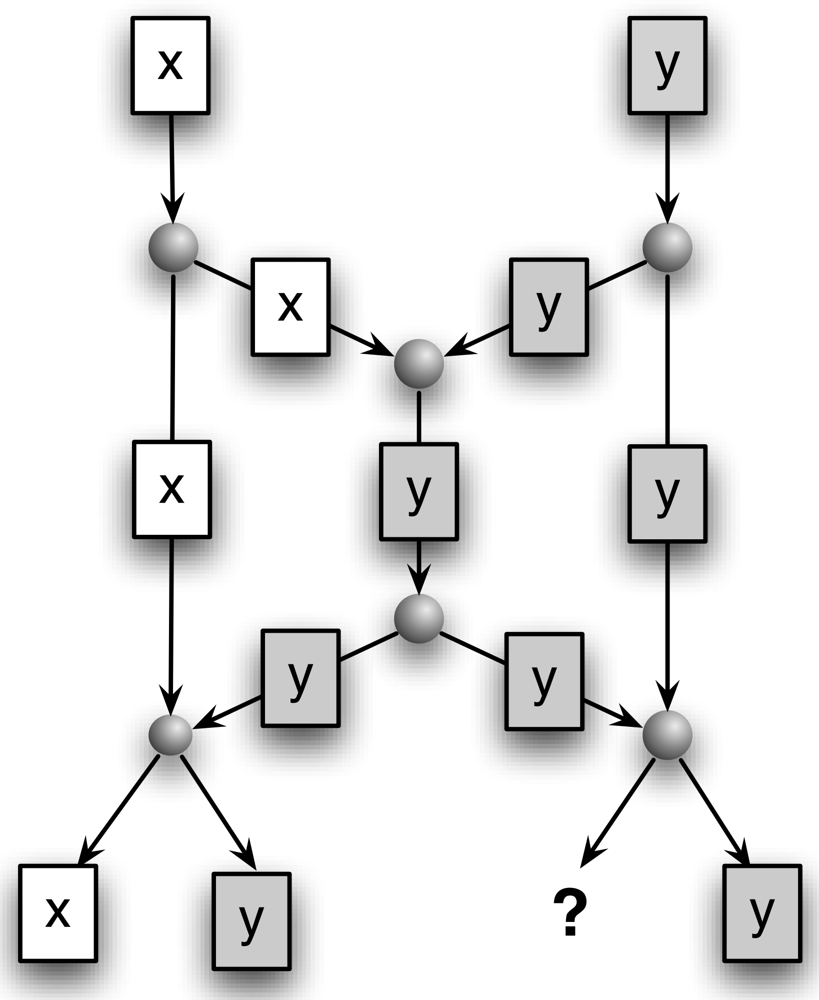
# Network Coding

- **R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung**
  - *Network Information Flow*, (IEEE Transactions on Information Theory, IT-46, pp. 1204-1216, 2000)
- **Example**
  - Bits x and y are to be transfered
  - Each edge carries only a bit
  - If bits are transfered as is
    - then both x and y cannot be received either on the left or right side



# Network Coding

- **Example**
  - Bits x and y are to be transfered
  - Each edge carries only a bit
  - If bits are transfered as is
    - then both x and y cannot be received either on the left or right side



# Network Coding

- **Solution**
  - Transfer Xor A+B on the middle edge

| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

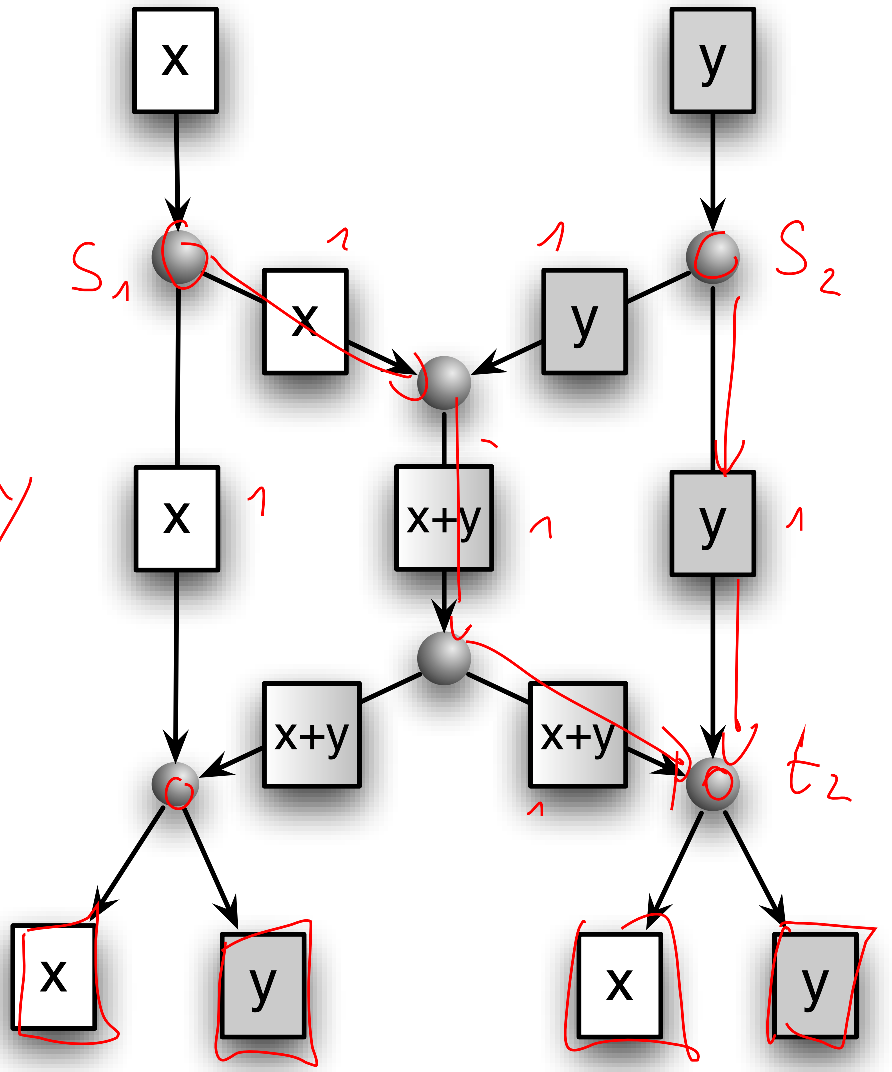
$x + x = 0$

$x + y = y + x$

$(x+y)+z = x+(y+z)$

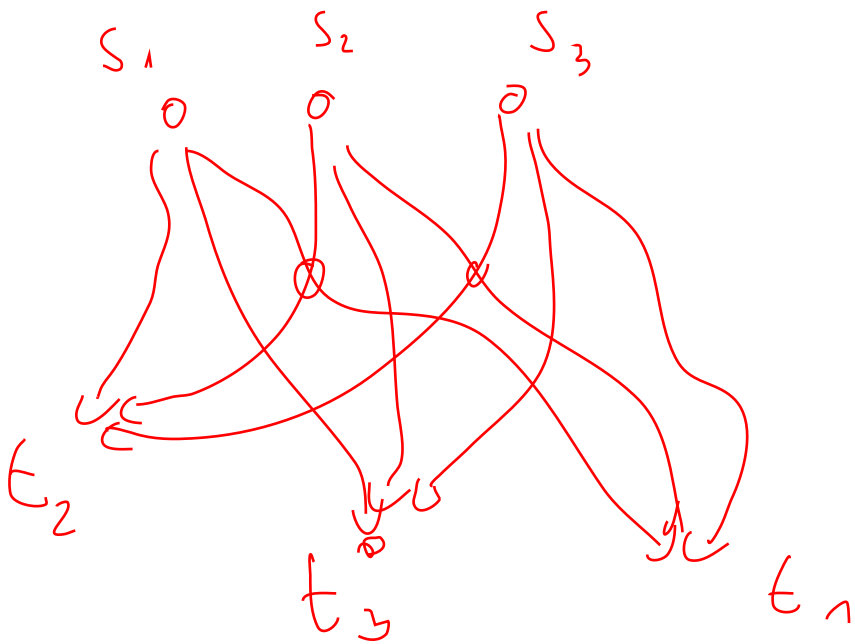
$\underbrace{x + x}_{0} + y = y$

$x + \underbrace{y + y}_{0} = x$



# Network Coding and Flow

- **Theorem [Ahlswede  et al.]**
  - For each graph there exists a network code such that each sink can receive as many bits as the maximum flow allows for each sink.



# Linear Codes for Network Coding

- **Koetter, Médard**
  - Beyond Routing: An Algebraic Approach to Network Coding
- **Task**
  - Efficiently compute the network code
- **Solution**
  - Linear codes can always solve network coding
- **Practical Network Coding**
  - With high probability even random linear combinations suffice

# Application Areas

- **Satellite Communication**
  - Preliminary work was published there
- **Peer-to-Peer networks**
  - Better information flow better than previous protocols
  - But too inefficient to displace prevalent protocols, e.g. Bittorrent
- **WLAN**
  - Xor in the Air, COPE
    - Simple network code improves flow
- **Ad-Hoc Networks, Wireless Sensor Networks, ...**

# Coding and Decoding

$y_i = x_1 \cdot r_{i1} + x_2 \cdot r_{i2} + \dots + x_m \cdot r_{im}$

- Original message: $x_1, x_2, \dots, x_m$
- Coding packet: $y_1, y_2, \dots, y_m$
- Random variable $r_{ij}$
- Then:

$$(r_{i1} r_{i2} \dots r_{im}) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = y_i$$

Random Matrix, message, code

$$\underbrace{\begin{pmatrix} r_{11} & \dots & r_{1m} \\ \vdots & \ddots & \vdots \\ r_{m1} & \dots & r_{mm} \end{pmatrix}}_{M} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$$

- If the matrix $(r_{ij})$ is invertable

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \underbrace{\begin{pmatrix} r_{11} & \dots & r_{1m} \\ \vdots & \ddots & \vdots \\ r_{m1} & \dots & r_{mm} \end{pmatrix}^{-1}}_{M^{-1}} \cdot \boxed{\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}}$$

$m$

$m^2$

# Inverse of a Random Matrix

- **Theorem**
  - If the numbers of an m x m Matrix are chosen randomly from a finite field with b elements, then the matrix is invertable with proability of at least

$$1 - \sum_{i=1}^{m} \frac{1}{b^i}$$

- **Idea: Consider Galois-Field GF[$2^k$]**
  - Computation is efficient
  - Binary represenation of data straight-forward

3 Bits → GF[$2^3$]

finite field

Boolean-Algebra = GF[$2^1$]

# Galois Field

- **GF($2^w$) = finite field with $2^w$ elements**
  - elements are binary strings of length w
  - 0 = $0^w$ neutral element of addition
  - 1 = $0^{w-1}1$ neutral element of multiplikation
- **u + v = bit-wise Xor of strings**
  - z.B. 0101 + 1100 = 1001
- **a b = product of polynomials modula a given irreducible polynomial and modulo 2**
  - i.e. $(a_{w-1} \ldots a_1\ a_0)\ (b_{w-1} \ldots b_1\ b_0)$ =

$$((a_0 + a_1 x + \ldots + a_{w-1}x^{w-1})(b_0 + b_1 x + \ldots + b_{w-1}x^{w-1}) \bmod q(x)) \bmod 2)$$

$\underbrace{0101110}_{w}$

$$\begin{array}{ll} 0101 & x \\ 1100 & y \\ \hline 1001 & x+y \end{array}$$

# Example: GF($2^2$)

$q(x) = x^2+x+1$

| Generator of GF(4) | Polynomial in GF(4) | Binary Represen-tation in GF(4) | Decimal Represen-tation |
|---|---|---|---|
| 0 | 0 | 00 | 0 |
| $x^0$ | 1 | 01 | 1 |
| $x^1$ | x | 10 | 2 |
| $x^2$ | x+1 | 11 | 3 |

$1+2=3$

$2+2=0$

$2\cdot 2=$

$1\cdot x^1 + 0\cdot x^0 = 10$

# Example: GF($2^2$)

| + | 0 = 00 | 1 = 01 | 2 = 10 | 3 = 11 |
|---|---|---|---|---|
| 0 =00 | 00 | 01 | 10 | 11 |
| 1 =01 | 01 | 00 | 11 | 10 |
| 2 =10 | 10 | 11 | 00 | 01 |
| 3 =11 | 11 | 10 | 01 | 00 |

# Example: $GF(2^2)$

$q(x) = x^2+x+1$

| * | 0 = 0 | 1 = 1 | 2 = x | 3 = $x^2$ |
|---|---|---|---|---|
| 0 = 0 | 0 | 0 | 0 | 0 |
| 1 = 1 | 0 | 1 | x | $x^2$ |
| 2 = x | 0 | x | $x^2$ | 1 |
| 3 = $x^2$ | 0 | $x^2$ | 1 | x |

$x^a \cdot x^b$

$= x^{(a+b) \bmod w-1}$

# Irreducible Polynomial

- **Irreducible polynomial cannot be factorized**
  - non- **Irreducible polynomial** $x^2+1 = (x+1)^2 \bmod 2$
- **Irreducible polynomials**
  - w=2: $x^2+x+1$
  - w=4: $x^4+x+1$
  - w=8: $x^8+x^4+x^3+x^2+1$
  - w=16: $x^{16}+x^{12}+x^3+x+1$
  - w=32: $x^{32}+x^{22}+x^2+x+1$
  - w=64: $x^{64}+x^4+x^3+x+1$

IEEE CRC

# Fast Multiplication

$2^8 \cdot 2^8 = 2^{16}$

$2^{16} \cdot 2^{16} = 2^{32}$

- **Power law**
  - Consider $\{2^0, 2^1, 2^2, \ldots\}$
  - $= \{x^0, x^1, x^2, x^3, \ldots$
  - $=$ exp(0), exp(1), ...
- **exp(x+y) = exp(x) exp(y)**
- **Inverse function: log(exp(x)) = x**
  - $\log(x \cdot y) = \log(x) + \log(y)$
- **x y = exp(log(x) + log(y))**
  - Caution: in the exponent standard addition
- **Tables store exponential function and logarithm**

# Example: GF(16)

= GF

$q(x) = x^4+x+1$

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| exp(x) | 1 | $x$ | $x^2$ | $x^3$ | $1+x$ | $x+x^2$ | $x^2+x^3$ | $1+x+x^3$ | $1+x^2$ | $x+x^3$ | $1+x+x^2$ | $x+x^2+x^3$ | $1+x+x^2+x^3$ | $1+x^2+x^3$ | $1+x^3$ | 1 |
| exp(x) | 1 | 2 | 4 | 8 | 3 | 6 | 12 | 11 | 5 | 10 | 7 | 14 | 15 | 13 | 9 | 1 |

| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| log(x) | 0 | 1 | 4 | 2 | 8 | 5 | 10 | 3 | 14 | 9 | 7 | 6 | 13 | 11 | 12 |

24 - 15

- $5 \cdot 12 = \exp(\log(5)+\log(12)) = \exp(8+6) = \exp(14) = 9$
- $7 \cdot 9 = \exp(\log(7)+\log(9)) = \exp(10+14) = \exp(24) = \exp(24-15) = \exp(9) = 10$

$a \cdot b = \exp(\log(a \cdot b)) = \exp(\log a + \log b)$

# Special Case GF[2]

- **Network Coding in GF[2]**
  - Boolean Algebra
    - $x + y =$ x XOR y
    - $x \quad y =$ x AND y
- **Example**
  - Xor in the Air
  - Multicasting in Ad-Hoc Networks
- **Disadvantage**
  - Full potential of network coding is unused
- **Advantage**
  - Transparent, intuitiv and very efficient

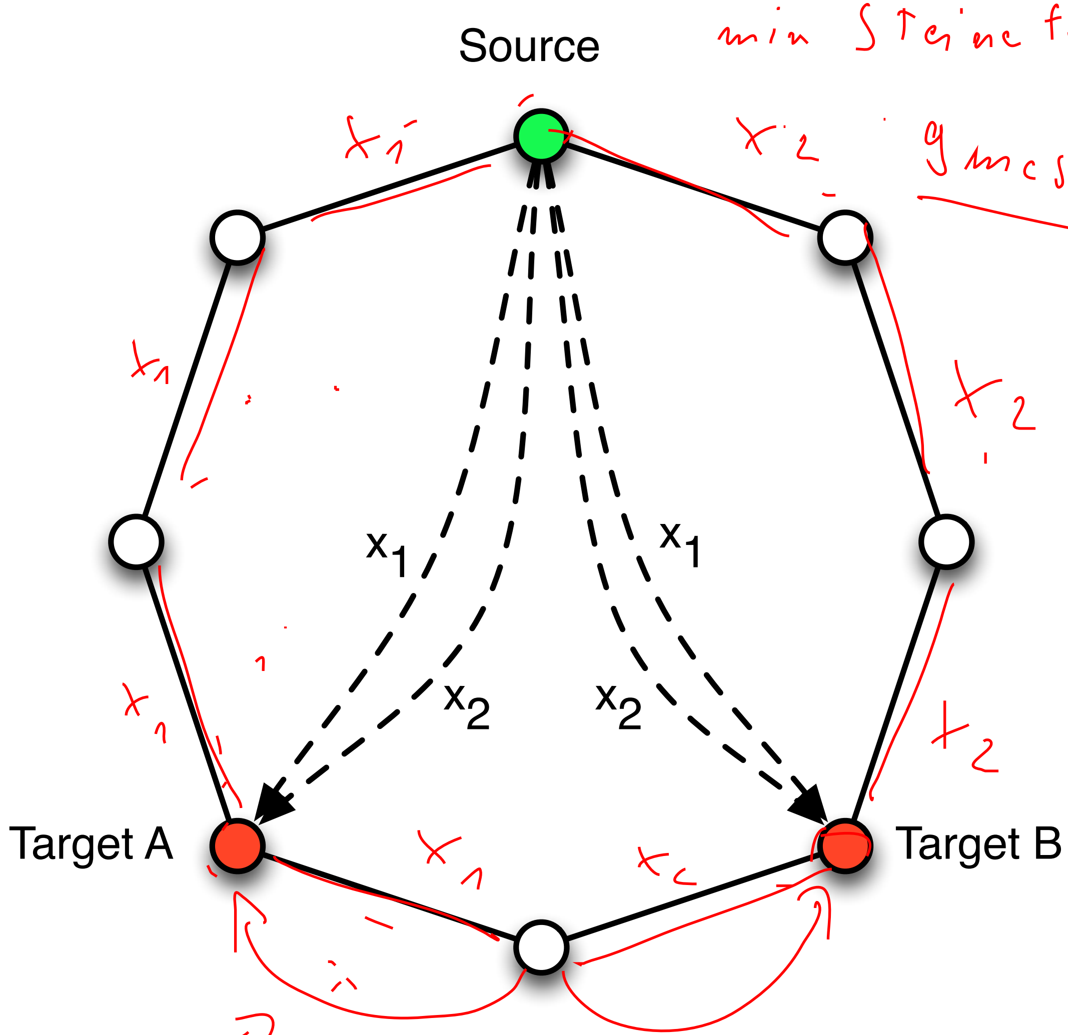
# Multicasting in Ad Hoc Networks

12 messages SPT

10 messages min Steiner tree

9 messages

- **Wu, Chou, Sun-Yuan,**
  - Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006
- **Multicast**
  - Distribute message from one node to a given set of nodes
- **Cost measure**
  - Each one-hop broadcast costs an energy unit

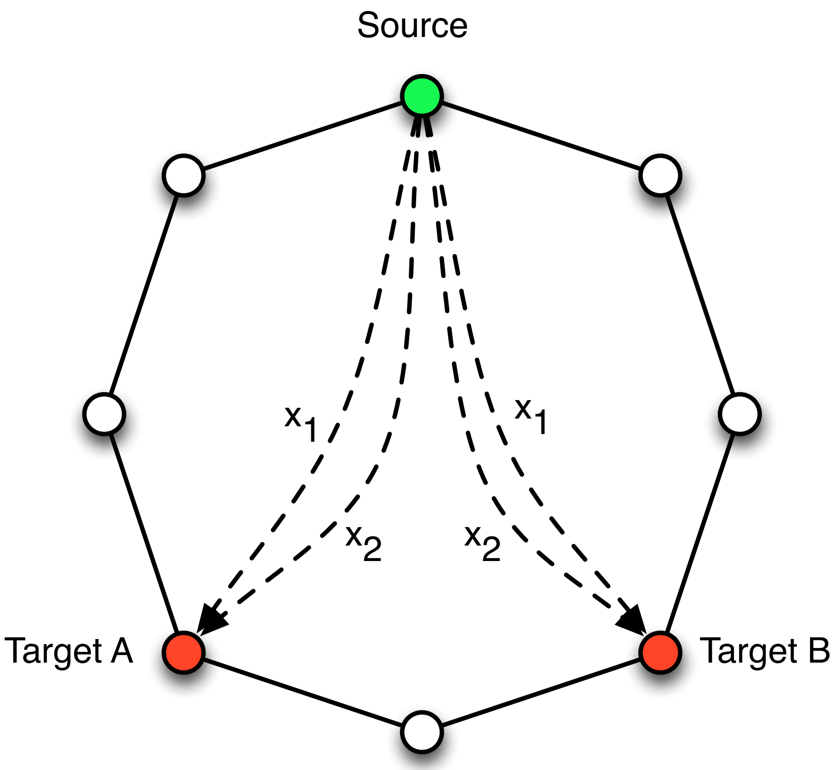


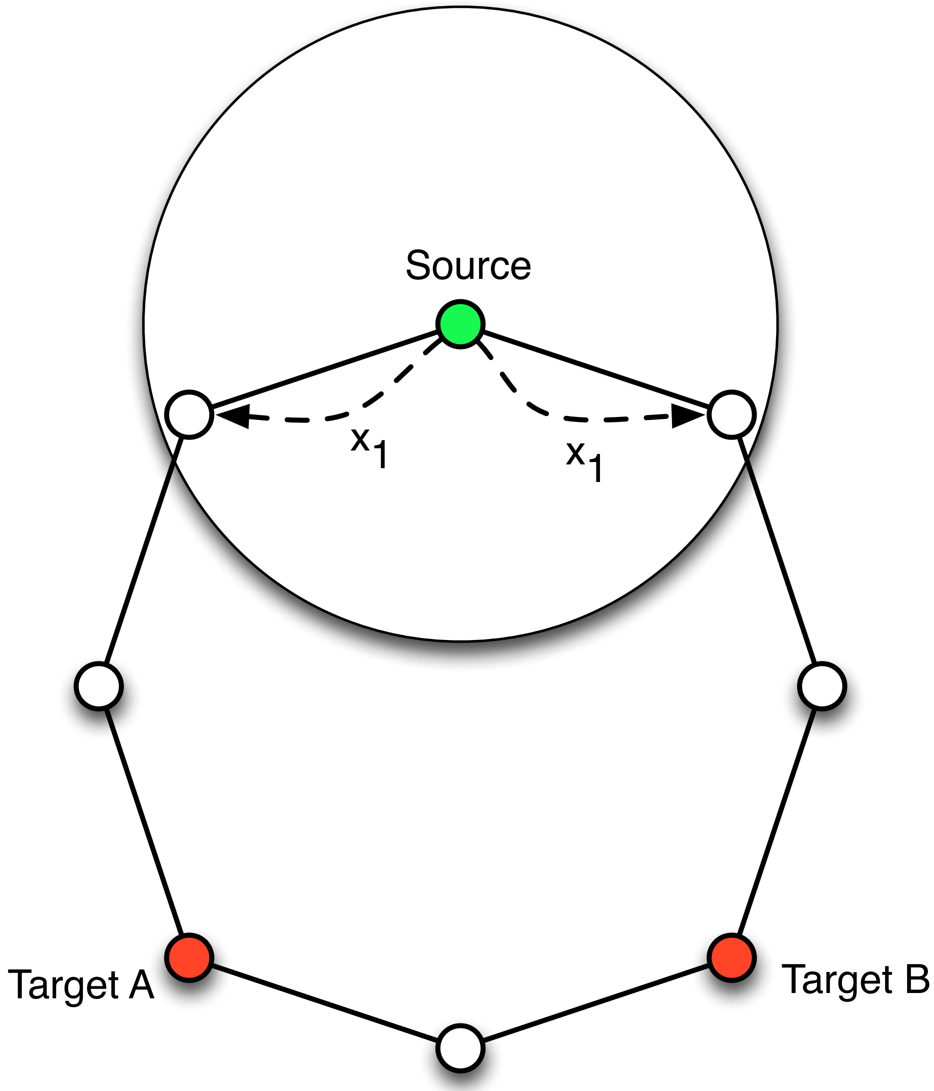

broadcast

$x_1 + x_2$

# Beispiel

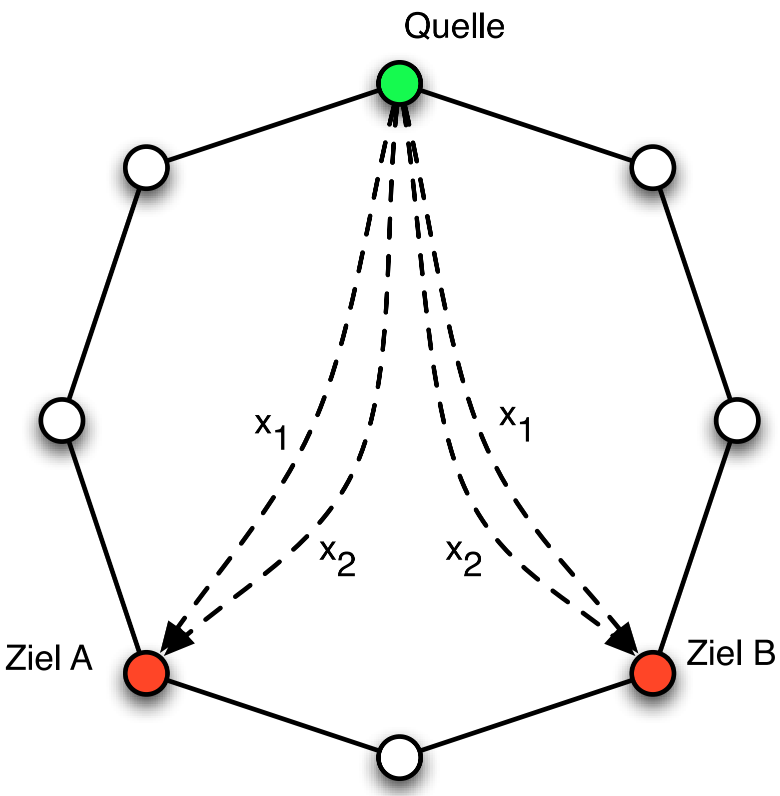
- **Traditionally,**
  - it costs 5 energy units for a multicast message

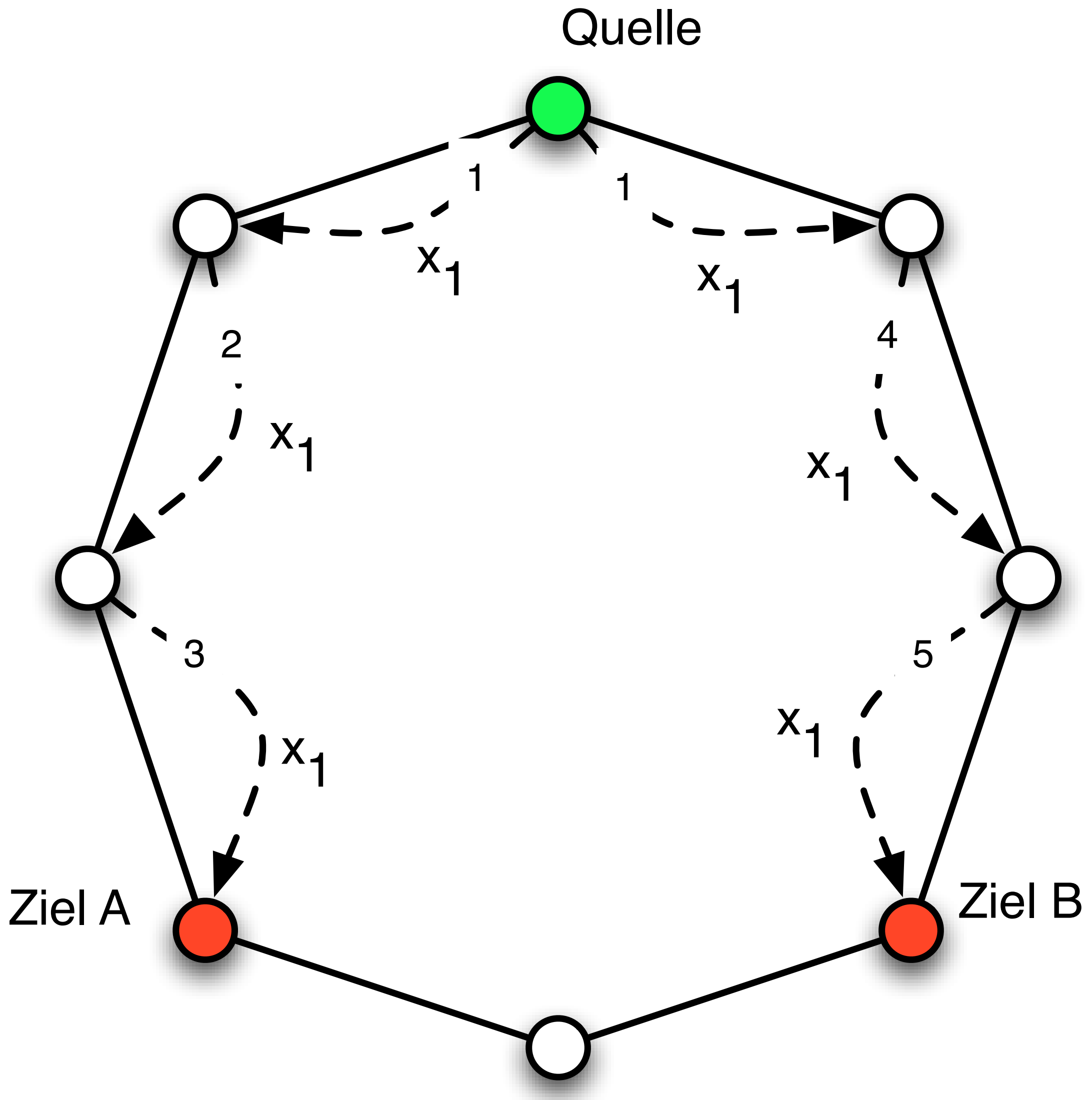


# Example

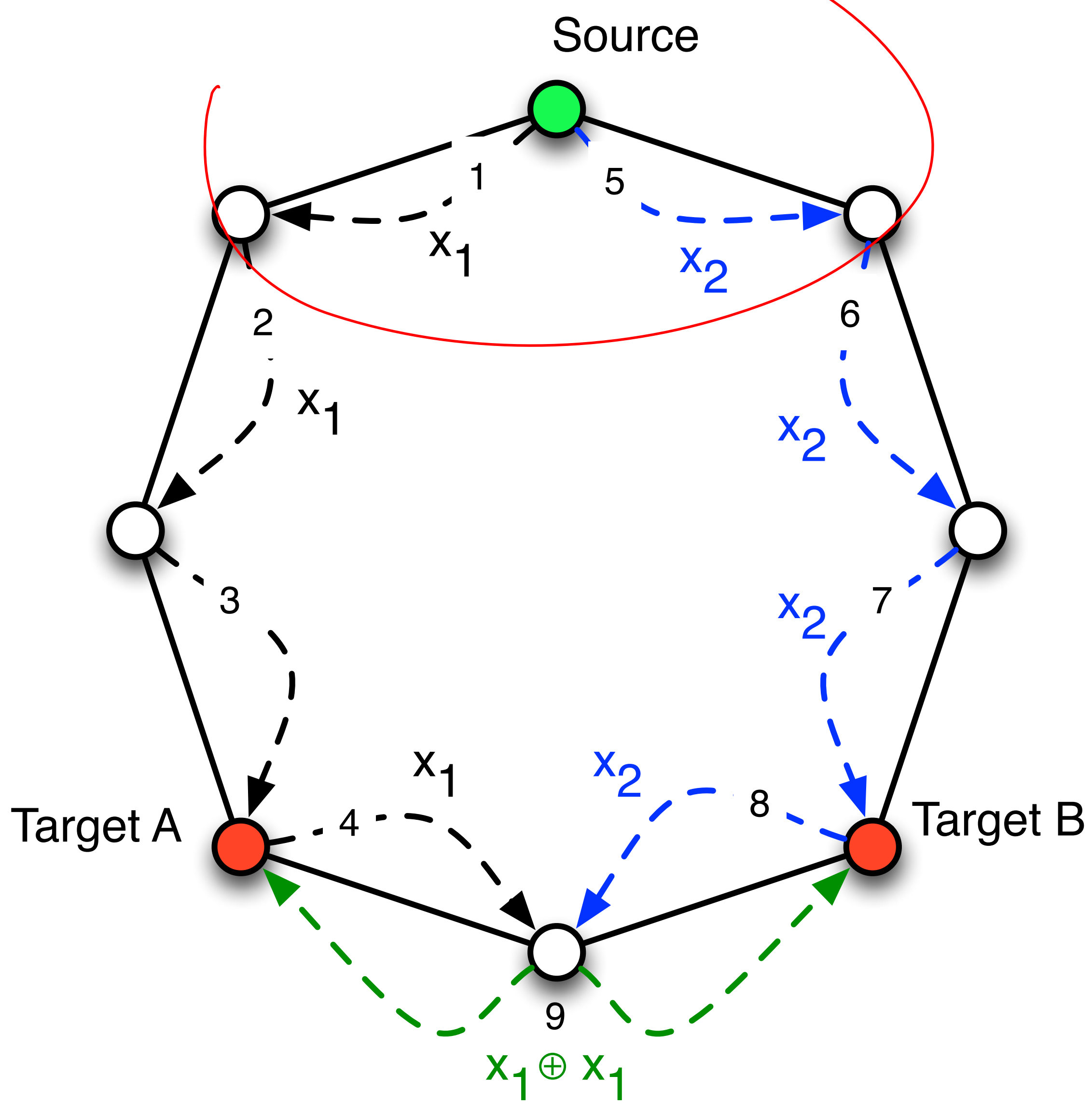
- **Traditionally,**
  - it costs 5 energy units for a multicast message



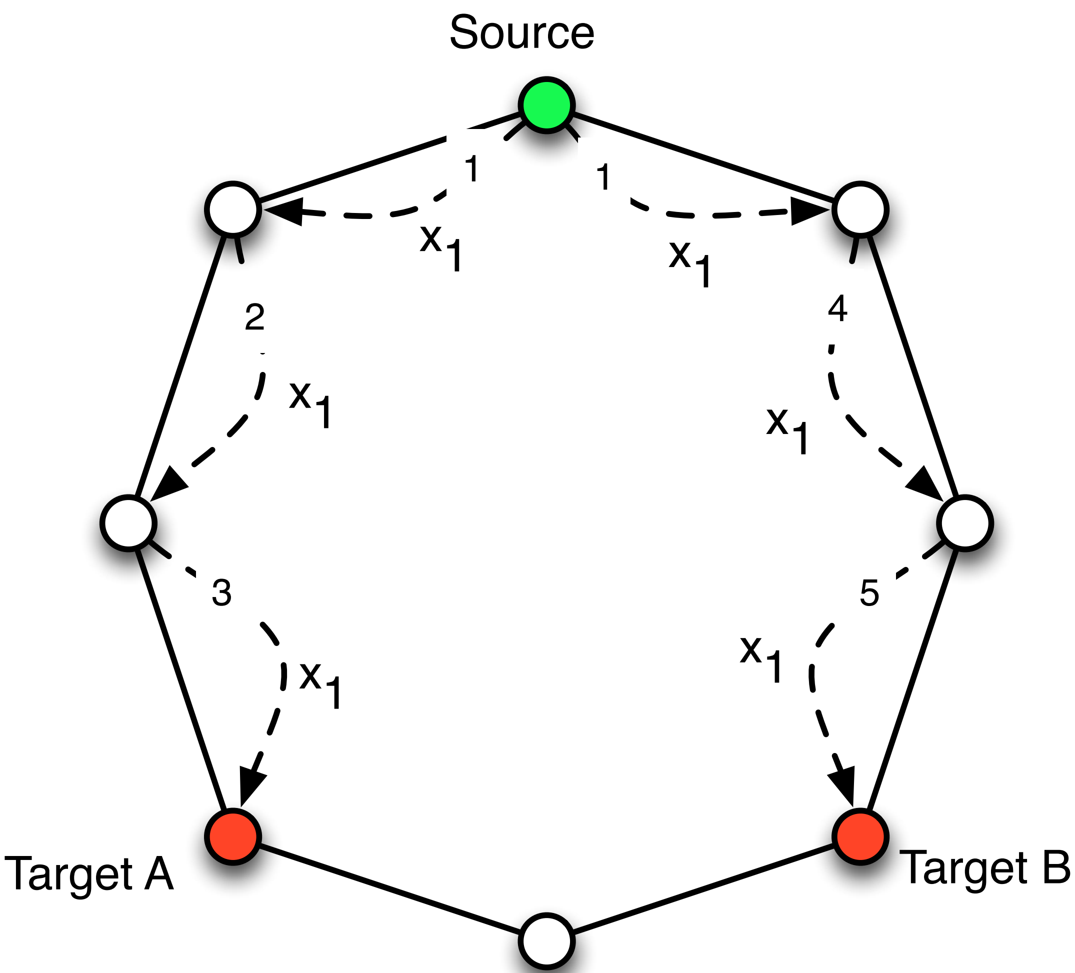
# Example

- **Network coding**
  - 9 energy units for 2 messages
  - Average of 4.5
- **Without network coding**
  - 5 units for one multicast message

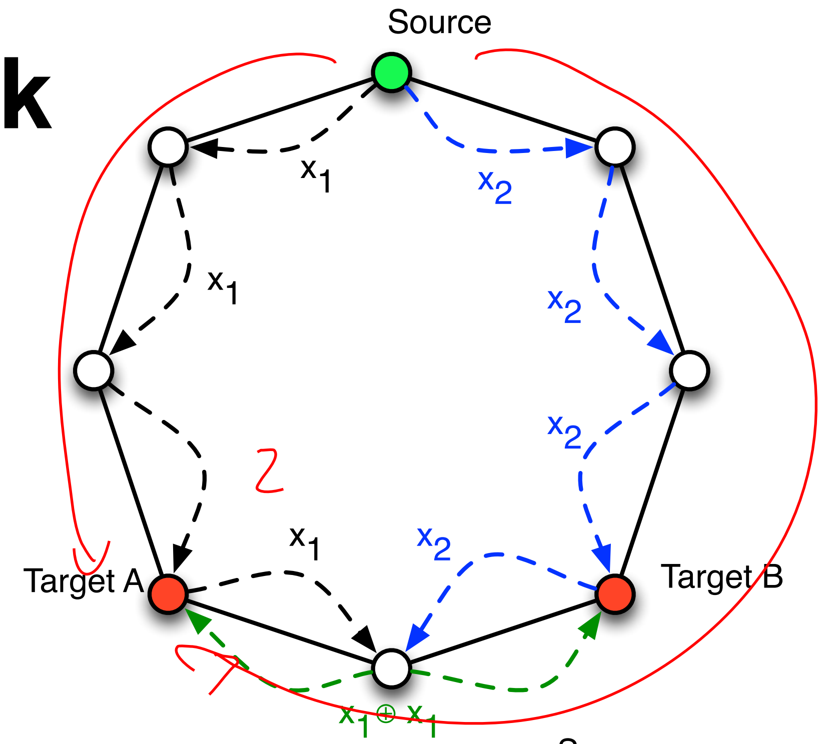


# Multicasting in Ad Hoc Networks

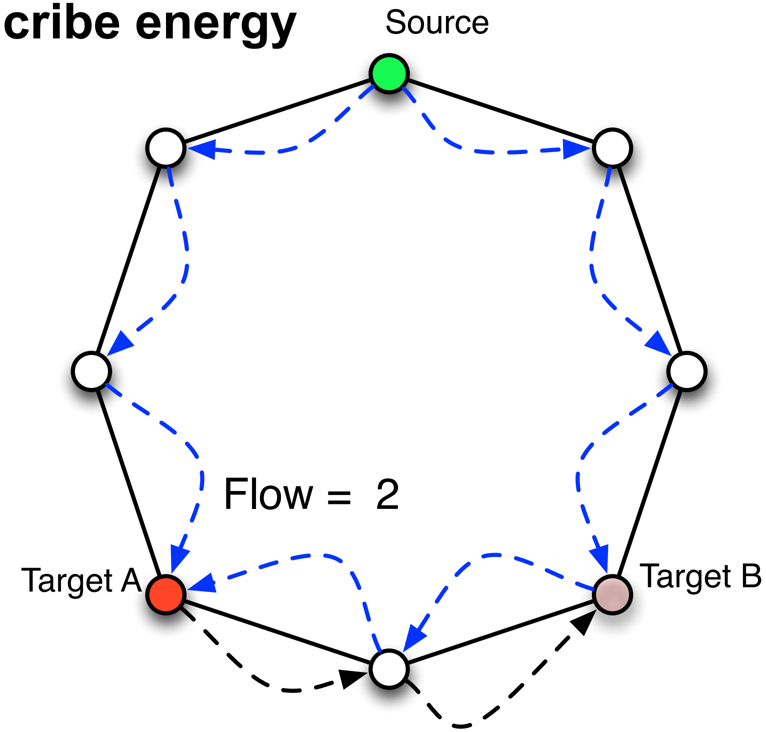
- **Solution of the minimal energy multicasting problem without network coding is NP-hard**
  - Less than constant factor approximation is NP-hard
  - Requires calculation of the discrete Steiner tree

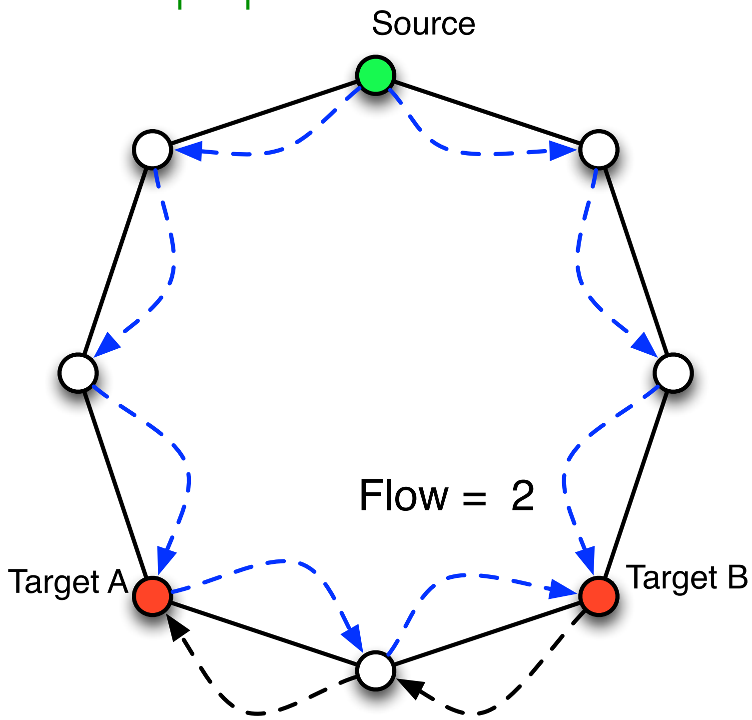


# Condition for Network Coding




- **Messages allow flow of the size of the desired number of messages**
  - from the sources to each individual sink
- **If such flows are guaranteed, network coding can be applied**
- **Size of the flows describe energy consumption**



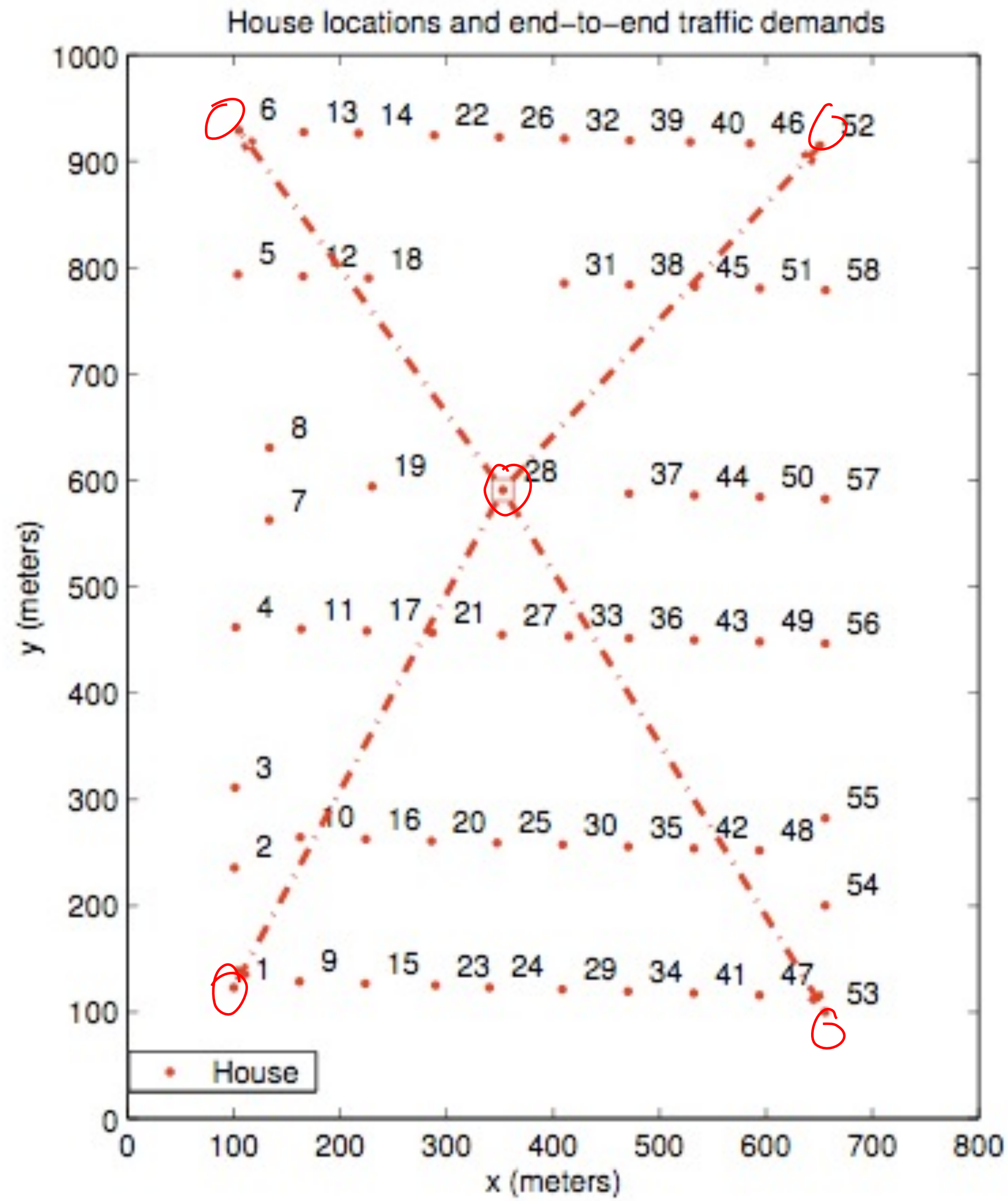
# Computational Complexity

- **Algorithm**
  - Collect all available link information
  - Formulate as linear program
  - Approximation of the solution
- **With the help of network coding, the maximum throughput can be approximated arbitrarily well in polynomial time**

$\boxed{\text{LS}}$

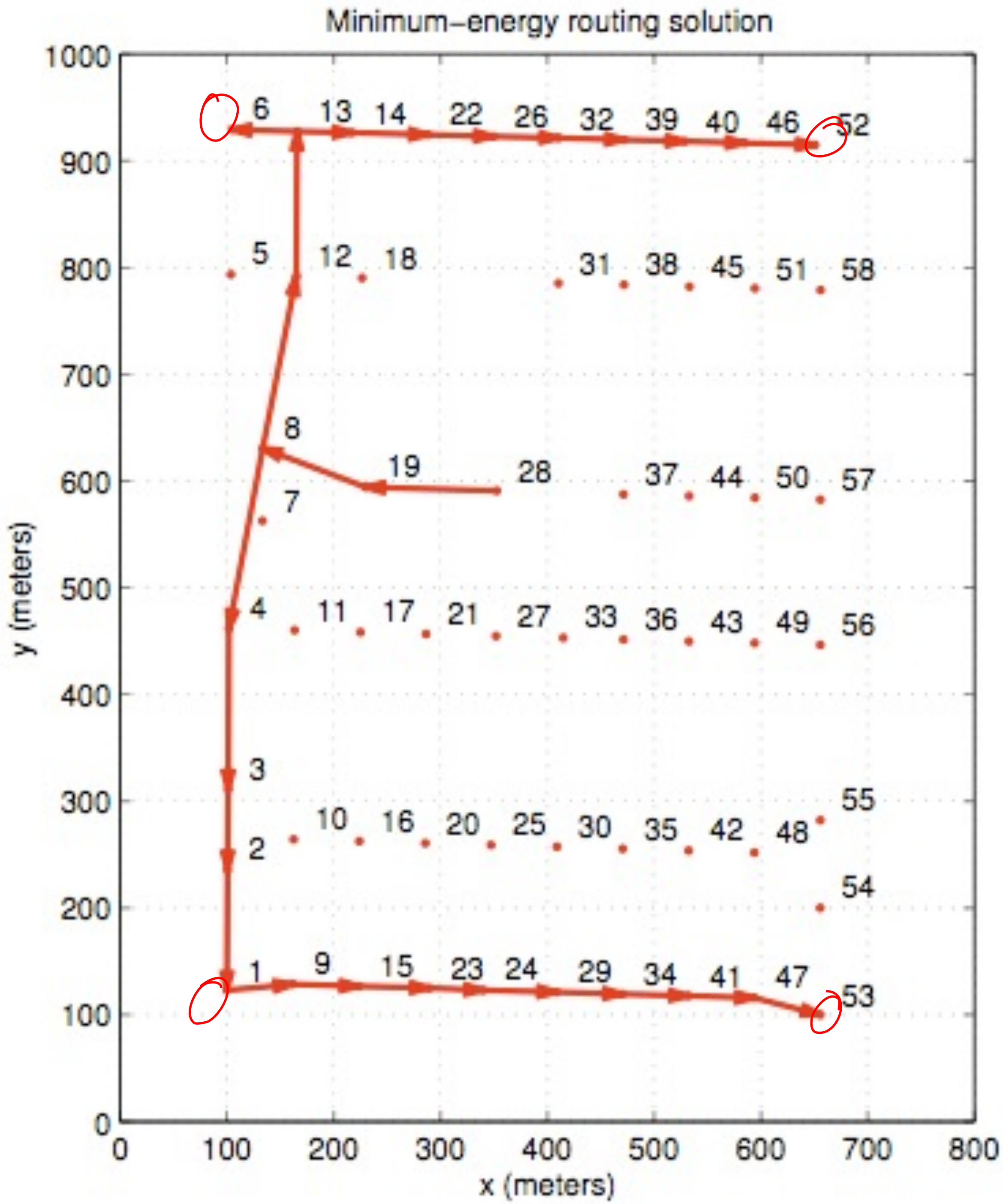
$\boxed{\text{Central}}$

# Example Demand



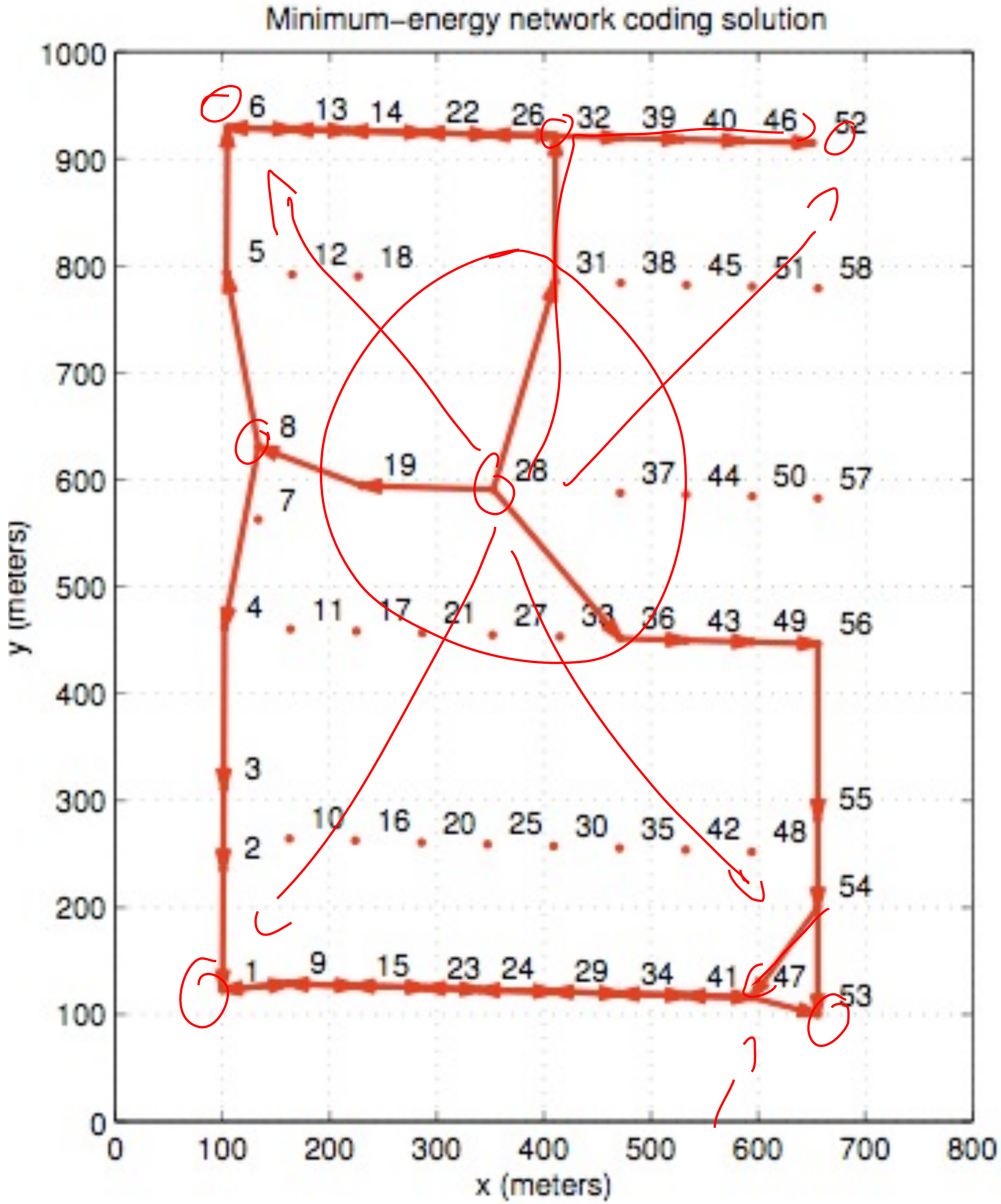

Wu, Chou, Sun-Yuan,
Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006

# Example Multicasting with minimal Energy




Wu, Chou, Sun-Yuan,
Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006

# Multicasting with Network Coding




Wu, Chou, Sun-Yuan,
Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006

# Discussion

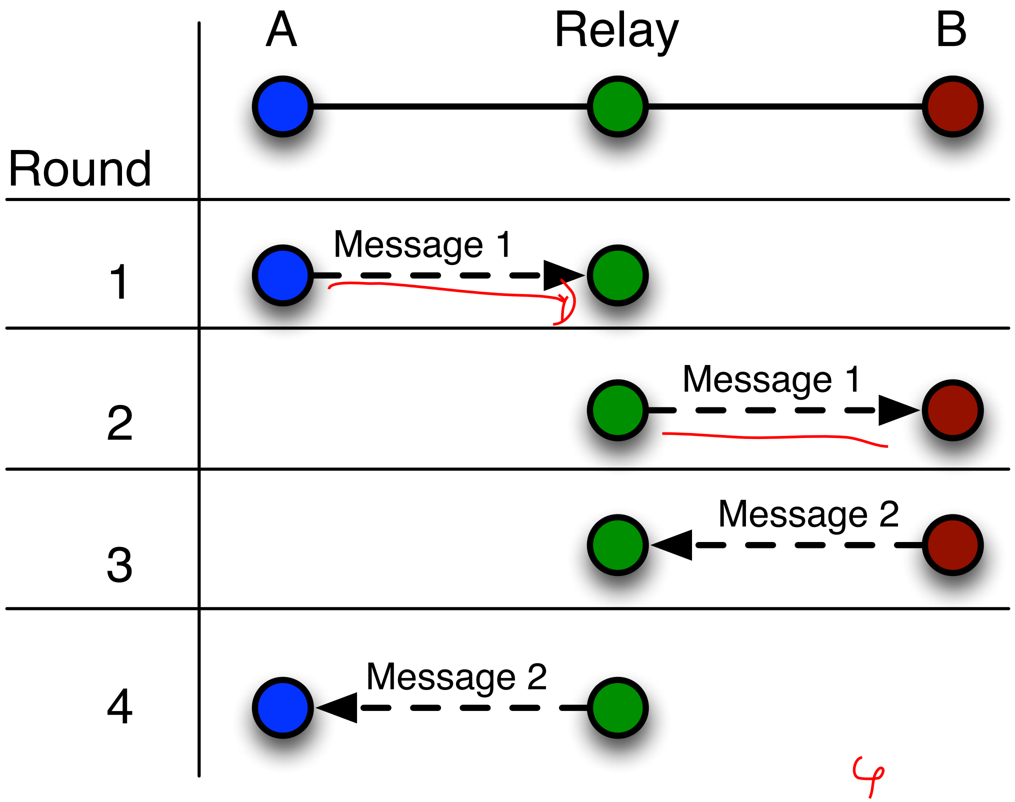
- **Options**
  - Energy model can customized
- **Limitations**
  - Network coding is not described
  - Central algorithm
  - Any change in the communication requires recalculation

# Xors in the Air

- **Katti, Hu, Katabi, Médard, Crowcroft**
  - XORs in the Air: Practical Wireless Network Coding
- **Problem**
  - Maximize throughput in ad-hoc network
  - Multihop messages cause interference
- **Solution**
  - Uses only XORs of multiple messages
  - Local, opportunistic algorithm

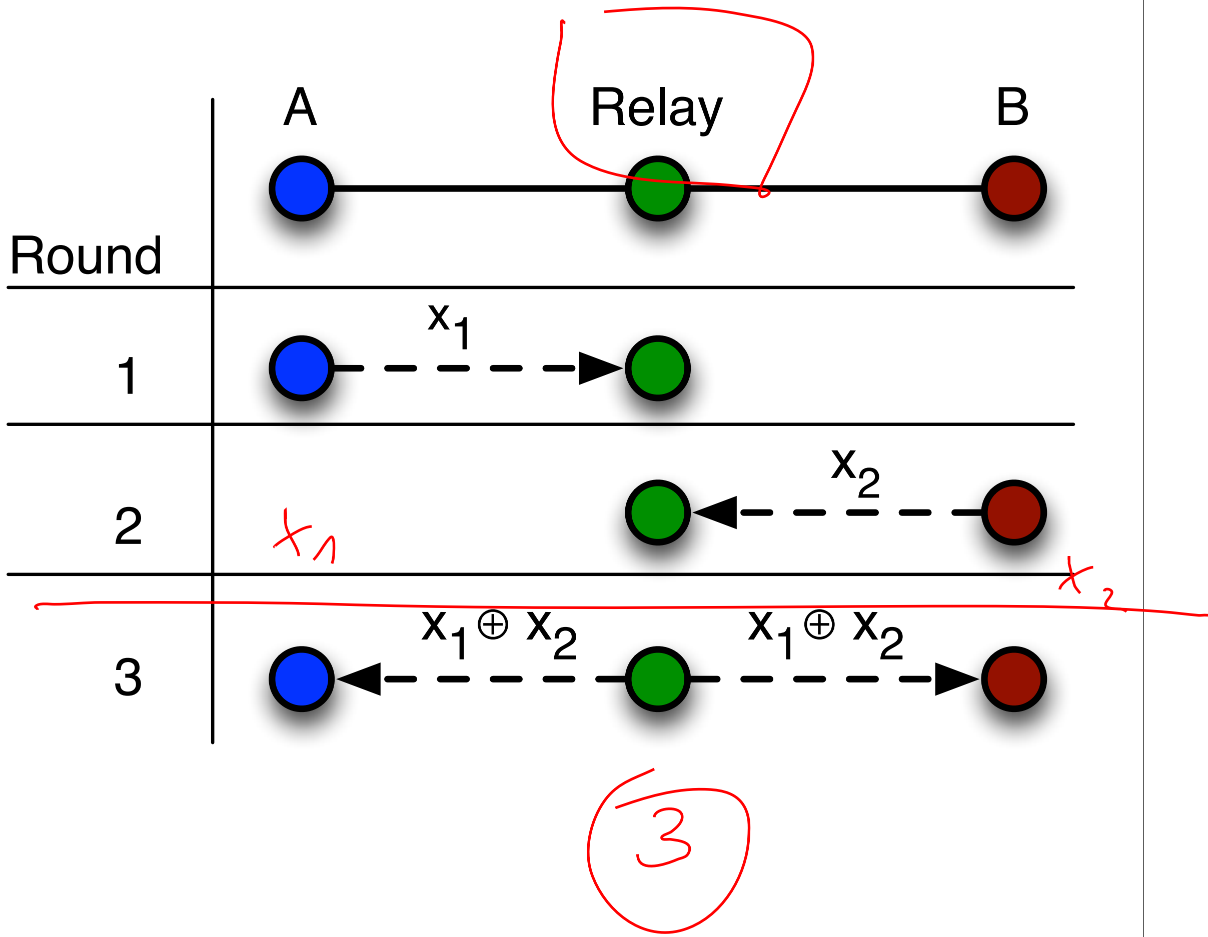
# Xors in the Air

- **Problem**
  - Multihop messages cause interferences
- **Example**
  - Traditional: 4 messages to send
    - a message from A to B
    - and a message from B to A



# Xors in the Air

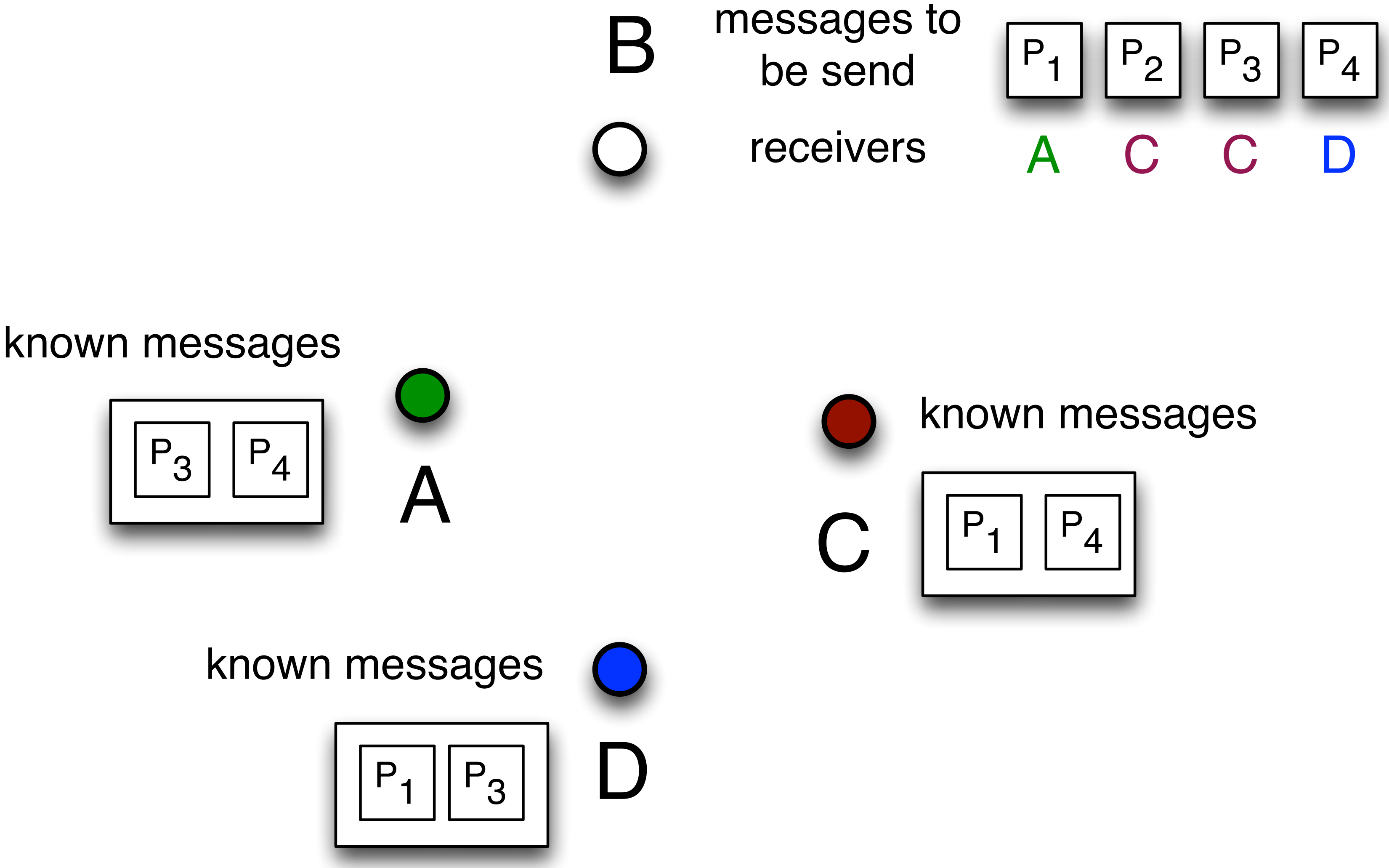
- **Problem**
  - Multihop messages cause interferences
- **Example**
  - Traditional: 4 messages to send
    - a message from A to B
    - and a message from B to A
  - Network Coding
    - 3 messages suffice



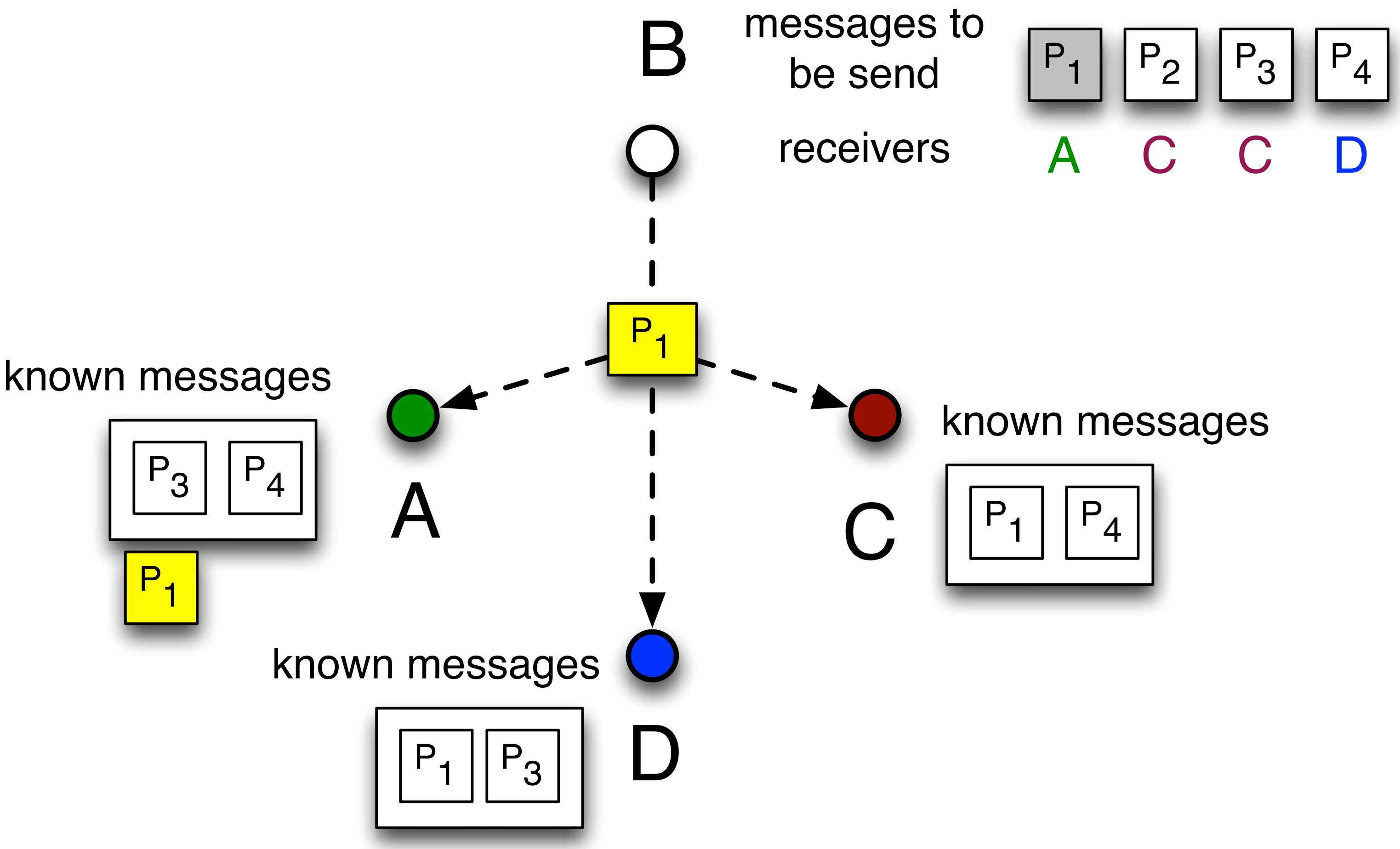
# Coding Opportunistically COPE

- **Consider of multiple communication paths**
  - Opportunistic coding of messages by Xor
- **Utilization of the broadcast medium**
  - listening to the channel
  - all (even foreign) messages are buffered
  - buffered messages are used for decoding
- **Context messages**
  - announcement of level of knowledge
  - neighbors can generate code adapted to the receiver's knowledge
- **Guess the level of knowledge of neighbors**

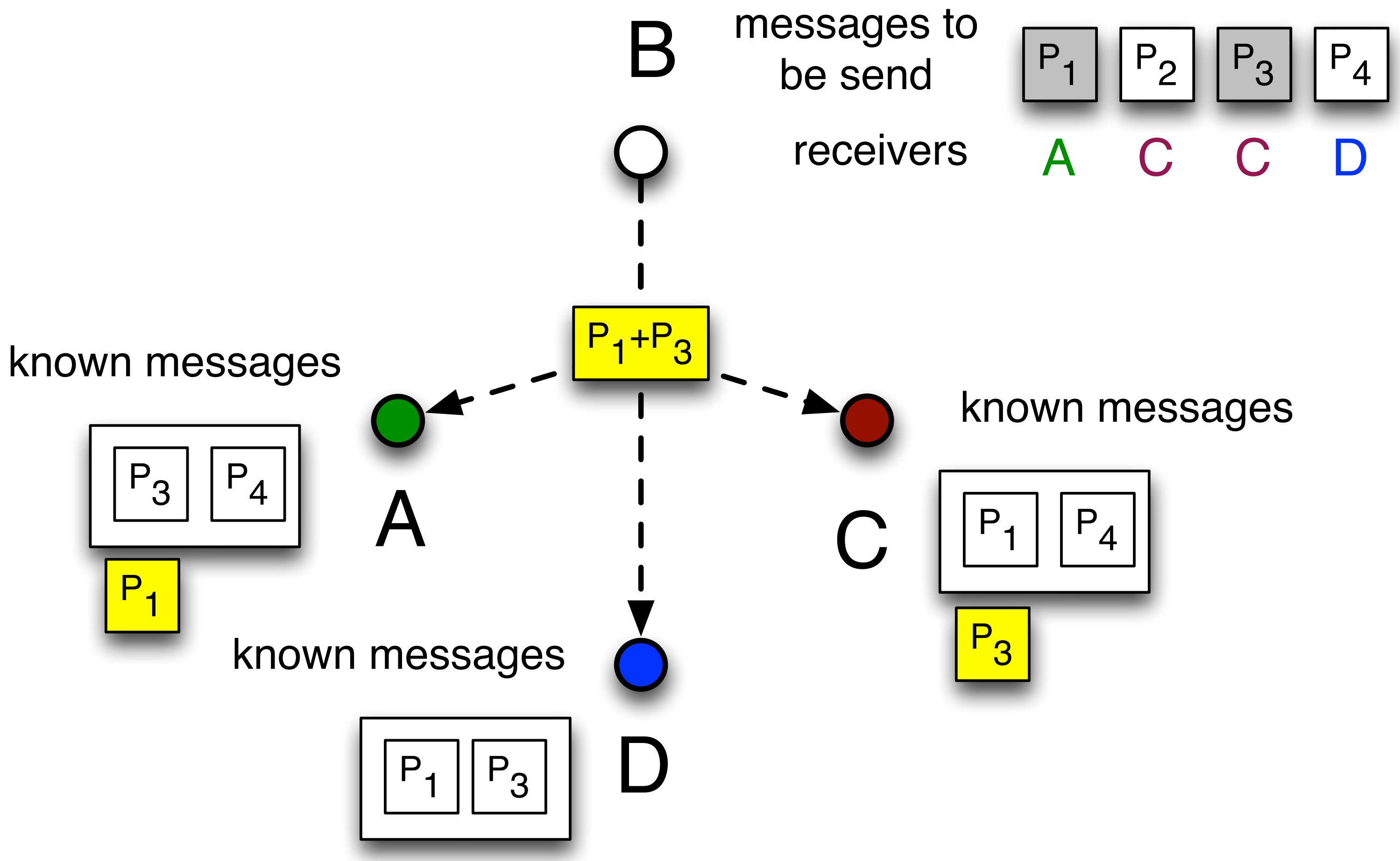
# Opportunistic Coding



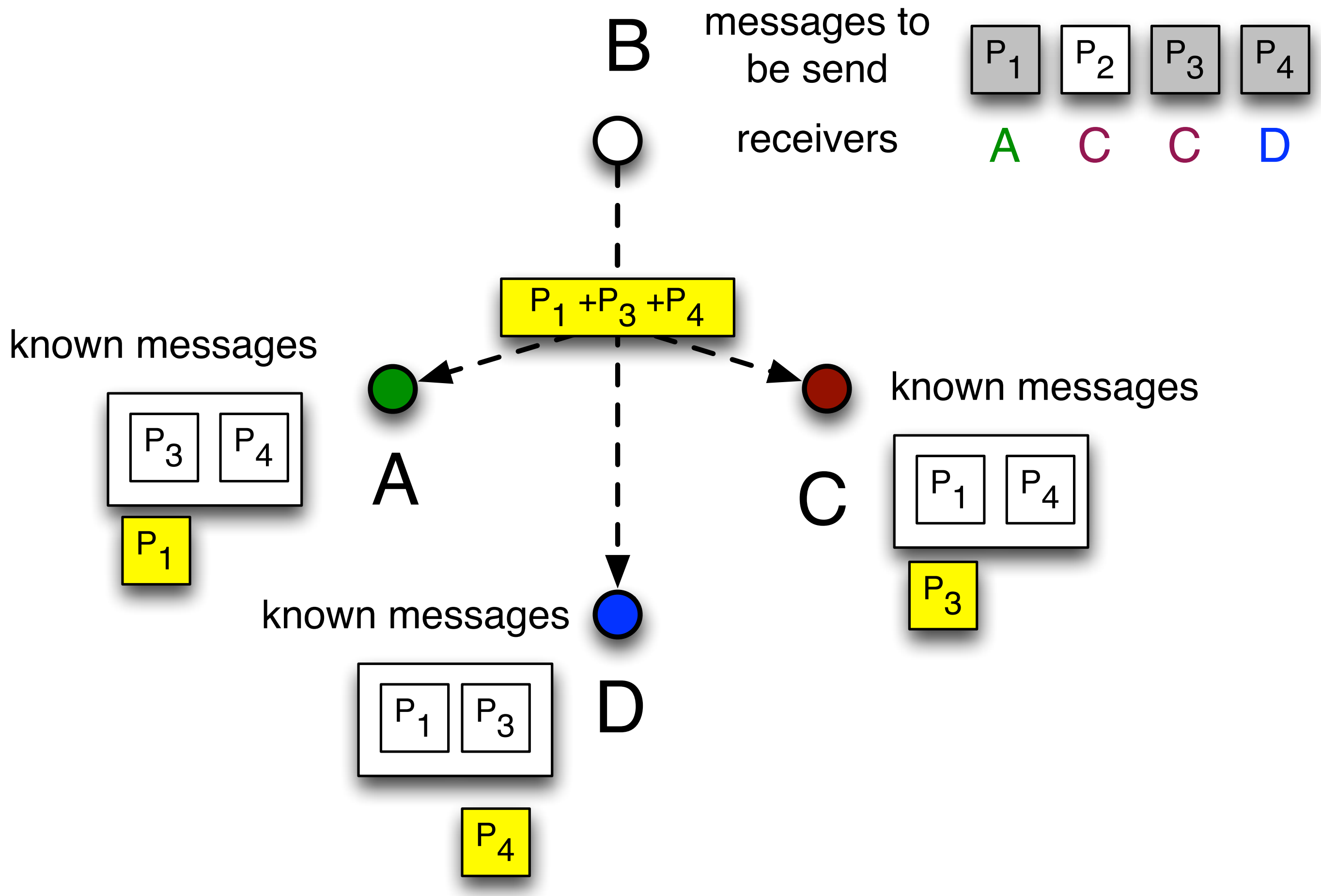
# Opportunistic Coding



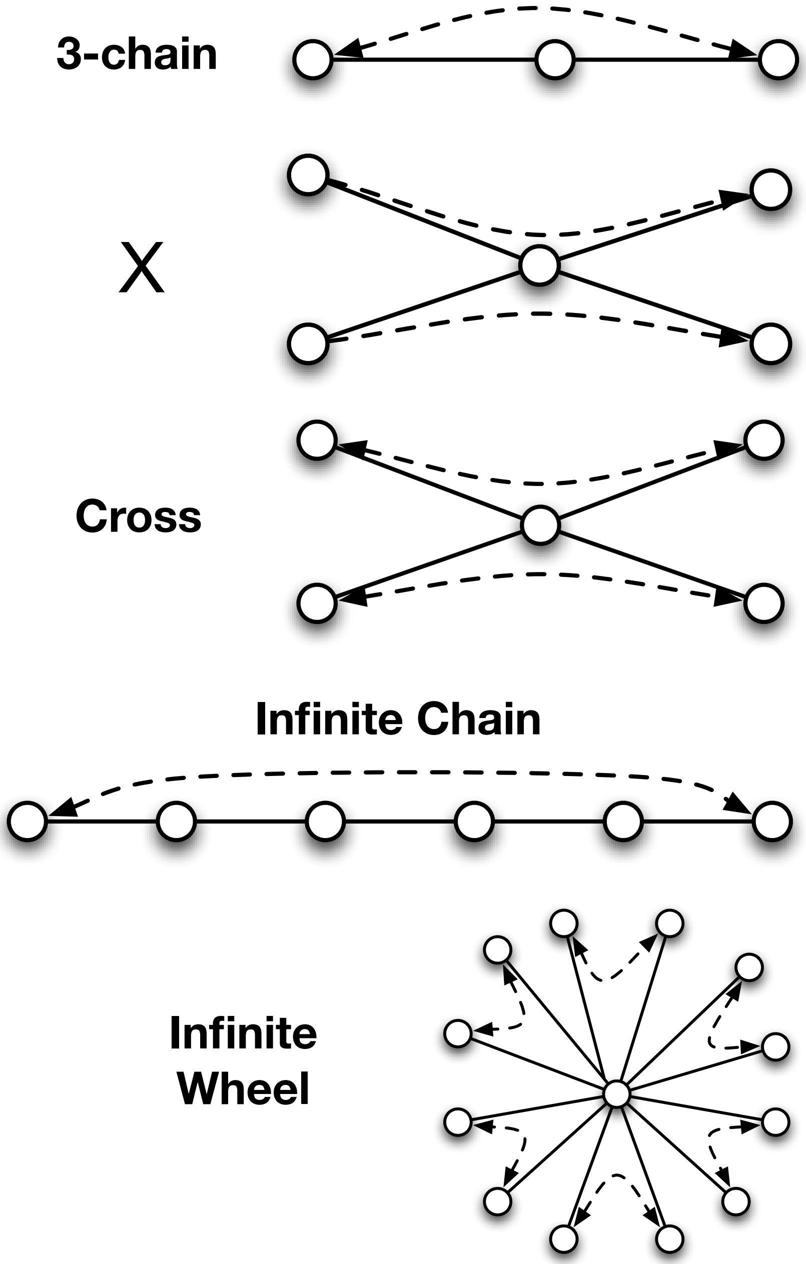
# Opportunistic Coding



# Opportunistic Coding



# Coding Gain




| Topology | Coding Gain |
|---|---|
| **3-chain** | 1,333... |
| **X** | 1,333... |
| **Cross** | 1,666... |
| **Infinite Chain** | 2 |
| **Infinite Wheel** | 2 |

# Summary Network Coding

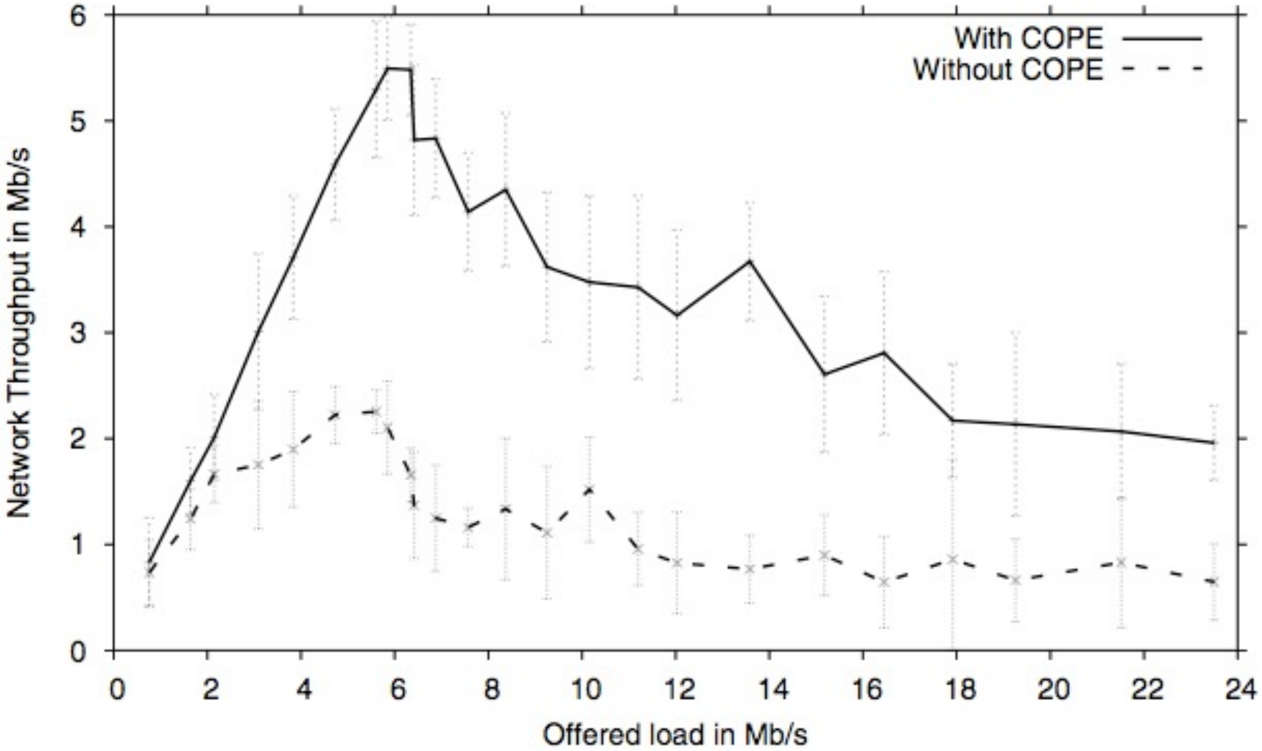



**Figure 12—COPE can provide a several-fold (*3-4x*) increase in the throughput of wireless Ad hoc networks. Results are for UDP flows with randomly picked source-destination pairs, Poisson arrivals, and heavy-tail size distribution.**

Wu, Chou, Sun-Yuan, Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006

# Network Coding

- **Benefit**
  - Network throughput can be increased
    - COPE
  - Reduction of energy consumption
  - Higher robustness, small error rate
  - Applications in peer-to-peer networks, wireless sensor networks
- **Problems**
  - complex encoding
  - sometimes high computational cost
  - difficult organization

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

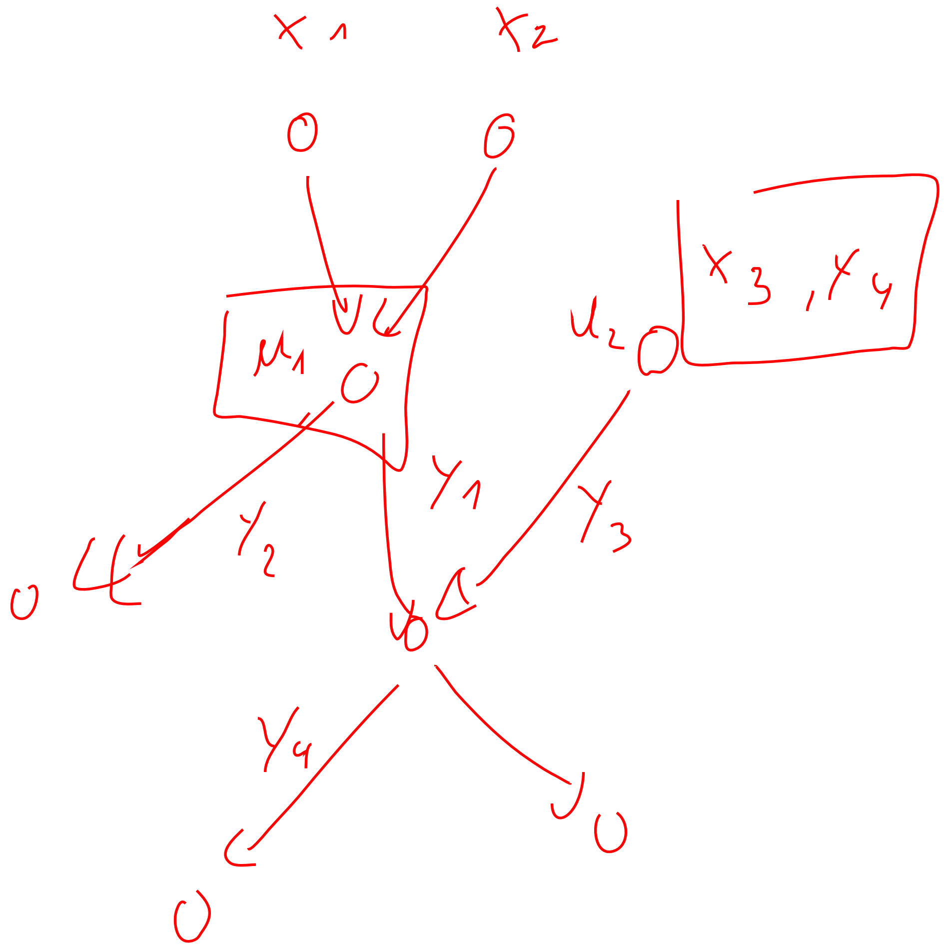
# Algorithms for Radio Networks

## Network Coding

University of Freiburg
Technical Faculty
Computer Networks and Telematics
Christian Schindelhauer

CoNe Freiburg

IIF




$$x_1 \cdot v_1 + x_2 \cdot v_2 = y_1$$

$$x_1 \cdot v_3 + x_2 \cdot v_4 = y_2$$

$$x_3 \cdot v_5 + x_4 \cdot v_6 = y_3$$

$$y_1 \cdot v_7 + y_2 \cdot v_8 = y_4$$

$$\overset{M}{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x+y \end{pmatrix}$$

$$M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$M = \begin{pmatrix} \boxed{1 \quad 0} \\ 0 \quad 0 \end{pmatrix} \qquad M^{-1} = \begin{pmatrix} \cdot\ ? \end{pmatrix}$$

$$\operatorname{rank}(M) = 1 \qquad M \cdot M^{-1} = \cancel{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}$$

$M'$

$$(n-1)\times(n-1)$$

0 ⋮ 0 ⋮ 0

$c$

decision

0 10111 0 011

$\operatorname{rank}(M') = n-1$

0 1
1 0
1 1

$\frac{1}{4}$

$n \to \infty$

$$P[\operatorname{rank}(M) = n] = \begin{cases} 1 \\ 0 \\ \text{constant} \\ \text{something else} \end{cases}$$

$n \times n$

$$\boxed{P[\operatorname{rank}(M) < n] \geq \tfrac{1}{2}}$$

$$\boxed{(\mathrm{mod}\ 7)}$$

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | | | | | | | |
| 4 | | | | ⋮ | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |

| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | | | |
| 4 | | | | | | … | |
| 5 | | | | | | | |
| 6 | | | | | | | |

$$2 \cdot 4 \equiv 8 \pmod{7}$$
$$\equiv 1$$

$$\boxed{\mathrm{RSA}}$$

$$GF[2] \qquad -1 = 1$$

| $+$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

| $*$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ |

---

| $-$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

$$0 - 1 = x \quad | +1$$

$$0 = x + 1 \quad | +1$$

$$1 = x + \underbrace{1 + 1}_{0}$$

$$1 = x$$

$$372 = 2 \cdot 10^0 + 7 \cdot 10^1 + 3 \cdot 10^2$$

$$372 \cdot 123 = 2 \cdot 3 \cdot 10^0 + 2 \cdot 2 \cdot 10^1 \ldots$$

$$(a_0 \cdot q^0 + a_1 q^1 \ldots)(b_0 \cdot q^0 \ldots) = \underline{\sum} \underline{a_i b_j} \cdot q^{i+j}$$

$$(c_u \cdot q^u + c_{u-1} q^{u-1} \ldots) : (d_w \cdot q^w + \ldots)$$

$$d_w \cdot q^u \ldots$$

CRC

$$x^2 + 1 = (x+1)^2 = x^2 + \underbrace{(x+x)}_{0} + 1$$

$$\boxed{x^2 + x + 1} =$$

$$x^2 = x \cdot x$$

```
10111 : 111 = 1010
111
-----
 101
 111
-----
  101
  111
-----
  0101
```

= 11011

$x^4 + x^3 + x + 1$ :

```
11011 : 111 = ~~10~~   Mod: 000
111
-----
 011
  111
  111
-----
  000
```